Regulatory & Compliance

Cyber Essentials Plus Policy

Document Information

Code:	**CD-CEP**	Created by:	**Steve Dodson**
Version:	**2.0**	Approved by:	**Lars Sneftrup Pedersen**
Date:	**28 June 2025**	Classification:	**Public**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2025 Admin By Request

San Francisco, Florida
Wisconsin, New York
(+1) 262 299 4600

Denmark, Norway,
Germany, Benelux
(+45) 55 55 36 57

United Kingdom, Spain
Switzerland, France
(+44) 20 3808 8747

Sweden, Thailand
Finland, New Zealand
(+46) 31 713 54 04

sales@adminbyrequest.com | support@adminbyrequest.com | www.adminbyrequest.com

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes the requirements for enforcing Single Sign-On (SSO) account separation within Admin By Request (ABR) for UK customers to ensure compliance with Cyber Essentials Plus.

The objective is to prevent privileged access using a primary account and enforce multi-factor authentication (MFA) for secondary accounts where applicable.

1.2 Scope

This policy applies to **all organizations in the UK** using ABR (Windows version 8.5.1 and later), requiring privileged access management (PAM). It further applies to any organization using ABR **outside the UK** that wishes to maintain compliance with Cyber Essentials Plus.

The scope includes:

- Users who require elevated permissions.
- IT administrators managing privileged access.
- Security and compliance teams enforcing Cyber Essentials Plus guidelines.

1.3 Definitions

The following definitions are used in this document:

- **User:** a person logging-in with standard privileges using a primary account.
- **Administrator:** a person logging-in with elevated privileges using a secondary account.
- **Primary account:** the main account used by a person for day-to-day activities.
- **Secondary account:** another account available to a person which has different (typically elevated) privileges from the primary account.

2 Policy Statement

2.1 Account Separation Requirements

Users must authenticate using a secondary SSO account before being granted administrative or elevated privileges.

The use of a single identity for both standard and privileged access is prohibited.

The MFA setting in ABR is enabled to enforce authentication using a secondary SSO account.

For UK customers, the SSO account separation setting is mandatory and enabled by default. For non-UK customers, this setting is optional and disabled by default.

If a user or administrator does not have two separate accounts, an alternative approach is possible in ABR, but this might not comply with Cyber Essentials Plus.

2.2 Authentication and MFA Enforcement

All users requesting privileged access must authenticate using MFA.

If a user does not have two separate accounts, an alternative approach may be applied:

- The user authenticates with minimum credentials (authentication or MFA) on the endpoint.
- The administrator must approve access via SSO to the ABR portal using a separate (i.e. secondary) account.
- This ensures that two distinct accounts are used in the process, though some auditors may interpret compliance differently.

2.3 Implementation in Admin By Request (ABR)

Organizations must update their Windows endpoints to ABR v8.5.1 to access the new MFA for secondary account setting.

IT administrators must configure the setting in the ABR portal and ensure users comply with the new authentication requirements.

The security team must verify that access control logs reflect proper account separation practices.

2.4 Compliance with Cyber Essentials Plus

This policy aligns with the Cyber Essentials Plus requirement that privileged access must be performed using a different account.

Organizations must maintain audit logs proving that two distinct accounts were used for privileged access approval.

If an alternative authentication approach is used, organizations must document and verify its acceptance with auditors.

2.5 Documentation and Review

A document outlining this policy (Cyber Essentials Plus Policy) is made available in the Documentation Center and/or the Trust Center, explaining compliance steps.

This policy shall be reviewed annually or upon updates to Cyber Essentials Plus or ABR functionality.

2 Document History

Version	Author	Changes
7 March 2025 **1.0**	Steve Dodson	Initial document release.
23 June 2025 **2.0**	Steve Dodson	Added "Documentation Center" (in addition to "Trust Center") as alternative location for this policy document. Applied latest template, aligned with Terms & Conditions and Data Processing Agreement documents.